2

Japanese Patent Laid-open Publication No.: 2001-14158 A

Publication date : January 19, 2001

Applicant : MITSUBISHI DENKI KABUSHIKI KAISHA

Title : CONTAMINATED PROGRAM DISTRIBUTION EXECUTING SYSTEM AND CONTAMINATED PROGRAM DISTRIBUTION EXECUTING METHOD

(57) [Abstract]

[Object] To provide a distribution executing system of a program for preventing illegal copying.

[Means] A program distributor transmits a contaminated program which is contaminated in advance and stored in a contaminated program storage unit 21 of a contaminated program distributing device 1, through a distributing unit 6. The program distributor encrypts decontamination information using a user's public key for distribution and transmits the encrypted decontamination information. The contaminated program is received by a contaminated program executing device 2 of a user and stored in a contaminated program storage unit 8. The received encrypted decontamination information is stored in an encrypted decontamination information storage unit 20. When the user executes the contaminated programs, the contaminated programs sequentially move to a program executing unit 9 to start execution. Simultaneously, a dynamic decontamination mechanism 10 activates to decrypt the encrypted decontamination information using a user's private key for reception, thereby decontaminating the contaminated part of the program by a decontaminator 16 using the decontamination information, just before the contaminated part of the program is executed.

[0003] As shown in Fig. 8, as long as the digital contents are distributed based on the "original data", it is difficult to completely regulate illegal copying. There is disclosed a technique in which "the distributed program is encrypted and the user that receives the encrypted program executes the program while dynamically decontaminating the program at its execution stage, thereby preventing illegal copying" in Japanese Patent Application Laid-Open No. S53-2541. In the conventional example, encryption is performed by code-converting the part of the operation code of the command in all the target programs. The inverse-conversion information for inversely-converting the converted operation code is stored in a dedicated ROM (Read Only Memory) provided in a CPU (Central Processing Unit) in a form of a conversion table. The distributor has to perform different encryption (operation code conversion) for different users and distributes the encrypted program, and to distribute decryption information (inverse-conversion information for the operation code) different for the different users in some way.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－14158
（P2001－14158A）
(43)公開日　平成13年１月19日(2001.1.19)

(51)Int.Cl.⁷	識別記号	Ｆ Ｉ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　9/06	５５０	Ｇ０６Ｆ　9/06	５５０Ｅ　５Ｂ０７６
			５５０Ｚ

審査請求　未請求　請求項の数10　ＯＬ　（全 14 頁）

(21)出願番号　特願平11－183597

(22)出願日　平成11年６月29日(1999.6.29)

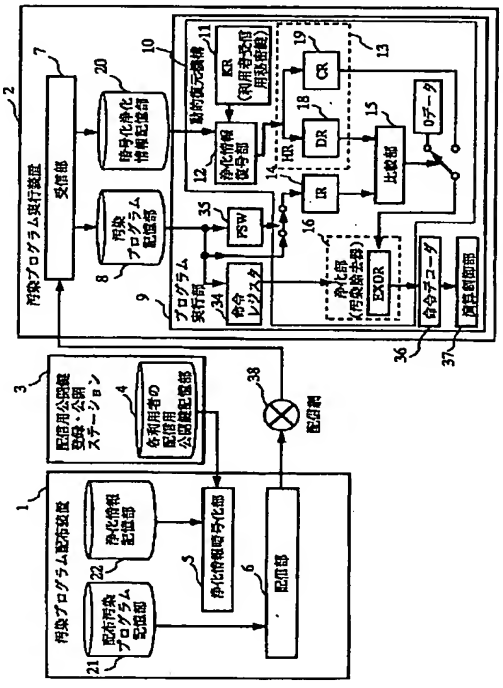
特許法第30条第１項適用申請有り　1999年１月26日　社団法人電子情報通信学会発行の「1999年暗号と情報セキュリティシンポジウム予稿集　ＶｏＬ．▲Ｉ▼ｏｆ▲ＩＩ▼」に発表

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　田窪　昭夫
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　曽我　正和
盛岡市盛岡駅西通り一丁目２番１－802号
(72)発明者　西垣　正勝
浜松市広沢一丁目23番１号
(74)代理人　100099461
弁理士　溝井　章司　（外２名）

Ｆターム(参考)　5B076 FA13

(54)【発明の名称】　汚染プログラム配布実行方式及び汚染プログラム配布実行方法

(57)【要約】
【課題】　不正コピーを防止するプログラムの配布実行方式を提供する。
【解決手段】　プログラム配布者は、汚染プログラム配布装置１の汚染プログラム記憶部２１に格納している予め汚染してある汚染プログラムを配信部６を通して送信するとともに、浄化情報を利用者の配信用公開鍵を用いて暗号化し暗号化浄化情報として送信する。汚染プログラムは、利用者の汚染プログラム実行装置２に受信され、汚染プログラム記憶部８に格納される。受信した暗号化浄化情報は、暗号化浄化情報記憶部２０に格納される。利用者が汚染プログラムを実行する場合、汚染された状態の汚染プログラムはプログラム実行部９に順次移り実行を開始する。同時に動的浄化機構１０が働いて利用者の受信用秘密鍵を用いて暗号化浄化情報を復号し、その浄化情報に基づいて汚染プログラムの汚染された部分が実行される直前に浄化部１６において汚染を除去され、実行される。



1

【特許請求の範囲】

【請求項１】　予めプログラムの所定の部分を汚染した汚染プログラムを配布する汚染プログラム配布装置と、上記汚染プログラム配布装置から配布された汚染プログラムを受信し、汚染プログラムを汚染されたまま実行開始するとともに、汚染された所定の部分を実行する場合に、汚染された所定の部分を汚染される元の状態に浄化して実行する汚染プログラム実行装置とを備えたことを特徴とする汚染プログラム配布実行方式。

【請求項２】　上記汚染プログラム配布装置は、
予め定められている汚染プログラムの汚染された所定の部分を汚染される元の状態に浄化するための浄化情報を、予め定められている利用者の公開暗号鍵を用いて暗号化する浄化情報暗号化部と、
汚染プログラムと浄化情報暗号化部が暗号化した浄化情報とを配信する配信部とを備えたことを特徴とする請求項１記載の汚染プログラム配布実行方式。

【請求項３】　上記汚染プログラム実行装置は、
汚染プログラムと暗号化された浄化情報とを汚染プログラム配布装置から受信する受信部と、
受信部が受信した汚染プログラムを記憶する汚染プログラム記憶部と、
受信部が受信した暗号化された浄化情報を記憶する暗号化浄化情報記憶部と、
汚染プログラム記憶部から汚染プログラムを入力して実行するプログラム実行部と、
暗号化浄化情報記憶部から暗号化された浄化情報を入力し、暗号化された浄化情報を復号するとともに、プログラム実行部の汚染プログラムの実行中に、浄化された浄化情報に基づいて、汚染プログラムの汚染された所定の部分を特定し、特定した所定の部分を浄化してプログラム実行部に実行させる動的浄化機構とを備えたことを特徴とする請求項２記載の汚染プログラム配布実行方式。

【請求項４】　上記動的浄化機構は、暗号化された浄化情報を復号するための復号鍵を記憶する受信用秘密鍵レジスタ（ＫＲ）と、
受信用秘密鍵レジスタ（ＫＲ）に記憶された復号鍵を用いて暗号化された浄化情報を復号する浄化情報復号部と、
浄化情報復号部により復号された浄化情報により復号された浄化情報を保持する浄化情報レジスタ（ＨＲ）と、
プログラム実行部により実行された実行情報を保持する実行情報レジスタ（ＩＲ）と、
浄化情報レジスタ（ＨＲ）に保持された浄化情報と実行情報レジスタ（ＩＲ）に保持された実行情報とを比較する比較部と、
比較部の比較の結果に基づいて、浄化情報を用いて汚染プログラムの汚染された所定の部分を浄化する浄化部とを備えたことを特徴とする請求項３記載の汚染プログラム配布実行方式。

2

【請求項５】　上記受信用秘密鍵レジスタ（ＫＲ）と上記浄化情報レジスタ（ＨＲ）と上記実行情報レジスタ（ＩＲ）は、上記レジスタが保持する内容を主記憶や他の装置へ読み出すことを不可能とすることを特徴とする請求項４記載の汚染プログラム配布実行方式。

【請求項６】　上記浄化情報は、
上記汚染された所定の部分の場所を特定する情報と、
上記汚染された所定の部分を浄化する情報とを備えたことを特徴とする請求項４記載の汚染プログラム配布実行方式。

【請求項７】　上記汚染された所定の部分の場所を特定する情報は、上記汚染された所定の部分の前に実行されるプログラムの命令語であり、上記実行情報レジスタ（ＩＲ）は、上記汚染された所定の部分の前に実行される命令語を保持することを特徴とする請求項６記載の汚染プログラム配布実行方式。

【請求項８】　上記動的浄化機構は、上記受信用秘密鍵レジスタ（ＫＲ）を除いて複数設けられ、複数の汚染プログラムが実行されることを特徴とする請求項３記載の汚染プログラム配布実行方式。

【請求項９】　或る一つのプログラムを独立複数の利用者のそれぞれのプログラム実行装置へ個別に配布する場合に、すべての利用者に対し同一の汚染を行った汚染プログラムと、汚染プログラムの汚染に対応する同一の浄化情報を各利用者が各個に保有する公開暗号鍵で各個に暗号化した暗号化浄化情報とを組み合せて配布することを特徴とする汚染プログラム配布実行方式。

【請求項１０】　予めプログラムの所定の部分を汚染した汚染プログラムを配布する汚染プログラム配布工程と、
上記汚染プログラム配布工程により配布された汚染プログラムを受信し、汚染プログラムを汚染されたまま実行開始するとともに、汚染された所定の部分を実行する場合に、汚染された所定の部分を汚染される元の状態に浄化して実行する汚染プログラム実行工程とを備えたことを特徴とする汚染プログラム配布実行方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】プログラムの不正コピー使用を無効化してプログラムを配布、実行するセキュア流通システム、特に、不正コピーを無効化するため意図的に汚染したプログラムの配布、実行する方式に関する。

【０００２】

【従来の技術】世界のディジタル社会化、特にインターネットの隆盛により、ディジタルコンテンツの流通が非常に活発となった。今後、電子商取引の基盤が整備され、ディジタルコンテンツの売買は、加速度的に増加していくであろう。ディジタル社会を実現する上で、著作権の保護に対する万全の対策・技術は不可欠である（郵政省監修：２１世紀の知的社会への改革、コンピュータ

エージ社、１９９４年）。特に問題となるのは、子コピー、孫コピーである。暗号化技術、スクランブル技術を用い、代金を支払った購入者にしかコンテンツをコピーさせないという方法（森亮一：ソフトウェアサービスシステムについて、電子通信学会誌、Ｖｏｌ．６７，Ｎｏ．４，１９８４年４月）を採っても、一度購入者にコンテンツが渡ってしまえば、その後のコピーを取り締まることはできない。これに対し、近年、ディジタル著作物にＩＤ（Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ ｎｕｍｂｅｒ）情報などを透かし情報として埋め込む電子透かし技術（Ｚｈａｏ，Ｊ．　ａｎｄＫｏｃｈ，Ｅ．：Ｅｍｂｅｄｄｉｎｇ Ｒｏｂｕｓｔ Ｌａｂｅｌｓ ＩｎｔｏＩｍａｇｅｓ Ｆｏｒ Ｃｏｐｙｒｉｇｈｔ Ｐｒｏｔｅｃｔｉｏｎ，Ｐｒｏｃｅｅｄｉｎｇｓ ｏｆ ＩＣＩＰＲ，１９９５）が脚光を浴びている。しかし、電子透かしは不正者を追跡する手段を提供するものであり、不正コピーを不可能にする技術ではない。また、電子透かしは、膨大なリダンダント情報を持つ画像には適用しやすいが、プログラムには適用しにくい。

【０００３】図８に示すように、ディジタルコンテンツの流通が「オリジナルデータ」をベースに考えられている限り、不正コピーを完全に取り締まることは難しいと言える。特開昭５３－２５４１に、「配信するプログラムを暗号化し、受信したユーザはそれを実行段階で動的に浄化しつつ実行する方法により不正コピーを防止する」という技術が開示されている。この従来例において、暗号化の方法は、対象プログラム中のすべての命令語のオペレーションコード部分をコード変換することである。変換されたオペレーションコードを浄化する為の逆変換情報は、変換表の形でＣＰＵ（ＣｅｎｔｒａｌＰｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）内に設けた専用ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）内に格納する。配布者は、異なる利用者毎に異なる暗号化（オペレーションコードの変換）を実施して配信し、何らかの方法で、利用者毎に異なる復号情報（オペレーションコードの逆変換情報）を配布せねばならないというものである。

【０００４】

【発明が解決しようとする課題】現在までに数多くの不正コピー防止技術が研究・開発されている。しかし、いまだ完全な不正コピー防止策は実現していない。以下に、主な従来技術とその問題点を検討する。まず、プログラムを暗号化して配信する技術を検討する。暗号化技術はプログラムを安全に配信することのみにその主眼が置かれているのが現状で、プログラム配信後のセキュリティに対しては効力を失ってしまう。即ち、正規の購入者にプログラムが暗号化され配信された後、購入者はそれを復号し、オリジナルデータの形でローカルマシンに保存することになる。クラッカーによりローカルマシンが攻撃され、このオリジナルデータが盗まれれば容易にプログラムは漏洩してしまうという問題がある。また、正規の購入者が悪意のあるユーザであった場合、自身が復号したオリジナルデータを無断で複製することは造作もないという問題がある。

【０００５】次に、パスワードによるチェックルーチンをプログラムに付加する技術を検討する。正規の購入者には、パスワードが知らされる。従って、購入者が悪意を持っていた場合、パスワードが漏洩し、プログラムは第三者に渡される可能性があり、実行可能となるという問題がある。また、プログラムを改造し、パスワードチェック部のルーチンをバイパスするという攻撃に弱いという問題がある。

【０００６】更に、電子透かしによって保護する技術では、暗号化技術を補完する技術として脚光を浴びているものの、電子透かしは不正者の追跡手段を提供するものである。従って、不正コピーの抑止力としては働くが、不正コピーを不可能にする技術ではないという問題がある。また、クラッカーが利用者のパソコンに侵入して電子透かし入りのコンテンツを盗み出して不正コピーを行うケースでは、透かしは利用者を示すことができるがクラッカーを特定することはできないという問題がある。

【０００７】更に、デバイス内のシステム管理領域など、エンドユーザには手の届かない部分にデータの一部を格納する技術では、デバイスのデッドコピーに弱く、計算機を熟知したクラッカーには対抗できないという問題がある。

【０００８】以上から、ディジタルコンテンツの流通が「オリジナルデータ」をベースに考えられている限り、完全なセキュア流通システムの実現は難しいと思われる。しかし、汚染コンテンツを流通するようにすれば、汚染コンテンツは不完全なディジタル情報であるので、クラッカーもしくは悪意のある購入者にコピーを取られたとしてもまったく支障がない。

【０００９】汚染コンテンツを流通させる方式で過去に発表されたものは、コンテンツ配布者が個別の利用者毎に異なる汚染を行うものである。その場合は、コンテンツを汚染する作業が利用者毎に必要となるため、配布に関わるコストが増大する。

【００１０】そこで、この発明は、ディジタルコンテンツの一部を意図的に破壊した「汚染コンテンツ」を一式だけ用意し、これを全ての利用者に配布することを基盤とするセキュア流通システムを構築することを目的とする。

【００１１】また、この発明は、利用者がオンライン／オフラインを通じ何らかの手段で配布者から購入し自己のパソコンに格納したプログラムについて、利用者がそれを正規に利用することはできるが、利用者がオリジナルコンテンツをコピーしたり、第三者へ配布することを防止する技術を確立することを目的とする。

【００１２】また、この発明は、クラッカーがインター

ネット上で、もしくは利用者のパソコンから、何らかの方法で該当プログラムを盗み出し、不正利用することを防止することを可能とする技術である。そこで、この発明は、プログラムの一部を意図的に汚染することにより、不正コピーを無効化する方法を提供することを目的とする。

【００１３】

【課題を解決するための手段】この発明に係る汚染プログラム配布実行方式は、予めプログラムの所定の部分を汚染した汚染プログラムを配布する汚染プログラム配布装置と、上記汚染プログラム配布装置から配布された汚染プログラムを受信し、汚染プログラムを汚染されたまま実行開始するとともに、汚染された所定の部分を実行する場合に、汚染された所定の部分を汚染される元の状態に浄化して実行する汚染プログラム実行装置とを備えたことを特徴とする。

【００１４】上記汚染プログラム配布装置は、予め定められている汚染プログラムの汚染された所定の部分を汚染される元の状態に浄化するための浄化情報を、予め定められている利用者の公開暗号鍵を用いて暗号化する浄化情報暗号化部と、汚染プログラムと浄化情報暗号化部が暗号化した浄化情報とを配信する配信部とを備えたことを特徴とする。

【００１５】上記汚染プログラム実行装置は、汚染プログラムと暗号化された浄化情報とを汚染プログラム配布装置から受信する受信部と、受信部が受信した汚染プログラムを記憶する汚染プログラム記憶部と、受信部が受信した暗号化された浄化情報を記憶する暗号化浄化情報記憶部と、汚染プログラム記憶部から汚染プログラムを入力して実行するプログラム実行部と、暗号化浄化情報記憶部から暗号化された浄化情報を入力し、暗号化された浄化情報を復号するとともに、プログラム実行部の汚染プログラムの実行中に、浄化された浄化情報に基づいて、汚染プログラムの汚染された所定の部分を特定し、特定した所定の部分を浄化してプログラム実行部に実行させる動的浄化機構とを備えたことを特徴とする。

【００１６】上記動的浄化機構は、暗号化された浄化情報を復号するための復号鍵を記憶する受信用秘密鍵レジスタ（ＫＲ）と、受信用秘密鍵レジスタ（ＫＲ）に記憶された復号鍵を用いて暗号化された浄化情報を復号する浄化情報復号部と、浄化情報復号部により復号された浄化情報により復号された浄化情報を保持する浄化情報レジスタ（ＨＲ）と、プログラム実行部により実行された実行情報を保持する実行情報レジスタ（ＩＲ）と、浄化情報レジスタ（ＨＲ）に保持された浄化情報と実行情報レジスタ（ＩＲ）に保持された実行情報とを比較する比較部と、比較部の比較の結果に基づいて、浄化情報を用いて汚染プログラムの汚染された所定の部分を浄化する浄化部とを備えたことを特徴とする。

【００１７】上記受信用秘密鍵レジスタ（ＫＲ）と上記浄化情報レジスタ（ＨＲ）と上記実行情報レジスタ（ＩＲ）は、上記レジスタが保持する内容を主記憶や他の装置へ読み出すことを不可能とすることを特徴とする。

【００１８】上記浄化情報は、上記汚染された所定の部分の場所を特定する情報と、上記汚染された所定の部分を浄化する情報とを備えたことを特徴とする。

【００１９】上記汚染された所定の部分の場所を特定する情報は、上記汚染された所定の部分の前に実行されるプログラムの命令語であり、上記実行情報レジスタ（ＩＲ）は、上記汚染された所定の部分の前に実行される命令語を保持することを特徴とする。

【００２０】上記動的浄化機構は、上記受信用秘密鍵レジスタ（ＫＲ）を除いて複数設けられ、複数の汚染プログラムが実行されることを特徴とする。

【００２１】この発明に係る汚染プログラム配布実行方式は、或る一つのプログラムを独立複数の利用者のそれぞれのプログラム実行装置へ個別に配布する場合に、すべての利用者に対し同一の汚染を行った汚染プログラムと、汚染プログラムの汚染に対応する同一の浄化情報を各利用者が各個に保有する公開暗号鍵で各個に暗号化した暗号化浄化情報とを組み合せて配布することを特徴とする。

【００２２】この発明に係る汚染プログラム配布実行方法は、予めプログラムの所定の部分を汚染した汚染プログラムを配布する汚染プログラム配布工程と、上記汚染プログラム配布工程により配布された汚染プログラムを受信し、汚染プログラムを汚染されたまま実行開始するとともに、汚染された所定の部分を実行する場合に、汚染された所定の部分を汚染される元の状態に浄化して実行する汚染プログラム実行工程とを備えたことを特徴とする。

【００２３】

【発明の実施の形態】実施の形態１．この実施の形態では、ディジタルコンテンツとして、実行形式のプログラムを一例として説明する。プログラムは、データの一部分、特に、そのメインルーチンのデータの一部分が汚染されれば、そのプログラムは正しく動作しなくなる。また、プログラムの汚染を除去、即ち、浄化する機構は、ＣＰＵに軽微の拡張を施すことにより付加することにより実現する。即ち、汚染プログラムは、実行の直前に拡張されたＣＰＵに備えられたプログラムの汚染を浄化する機構によって汚染が浄化され、正しく実行する。このように、静的状態でのデータ浄化を一切行わず、実行の瞬間にデータを浄化することを「動的浄化」とする。従って、プログラムは、ファイルされている期間はもちろんのこと、主記憶にロードされた段階においても汚染されたままである。このようにして、この発明は、オリジナルプログラムは、いかなる記憶装置上にも残さないようにする技術を提供する。具体的には、後述する。

【００２４】また、プログラムは、インターネットやＣ

7

Ｄ－ＲＯＭ（Ｃｏｍｐａｃｔ　Ｄｉｓｃ　Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）などによりオンライン／オフラインを通じて配布される実行形式のプログラムであり、配布を受けたユーザは二次加工を行わないことを前提とする。また、実行形式プログラムを逆アセンブルしてソースプログラムを得るには膨大な労力を要し、経済的に引き合わないことを前提とする。プログラムは、命令語を有することを前提とする。汚染されてないプログラムをオリジナルプログラム、または、単にプログラムという。また、命令語と命令は同じものを示している。更に、命令語は、インストラクションコードともいう。この実施の形態では、オリジナルプログラムの命令Ｘを汚染し、汚染命令Ｚを生成する場合を説明する。

【００２５】次に、汚染とは、コンテンツ（この実施の形態では、配布対象となるプログラム）の実効的価値、または商品的価値を意図的に損なうことを目的として、配布対象となるプログラムに加える変形をさす。具体的には、命令語を破壊することを特徴とする。特に、この実施の形態では、命令語のオペランドを破壊し、プログラムが正常な動作を実行し得ない場合を一例として取り上げる。しかしながら、汚染は、オペランドの破壊に限るものではなく、また、命令語を破壊するという汚染の方式に限るものではないことはいうまでもない。コンテンツの価値を損なう方法であれば、この他の汚染方法でも構わない。更に、汚染とは、コンテンツ（配布対象となるプログラム）を破壊するという点で、コンテンツの価値を損わないように加工を加える電子透かし、或いは、暗号化、符号化、圧縮化とは全く異なるものである。

【００２６】以下の説明では、コンテンツの取り引きにおける三者を次のように名付ける。ディジタルコンテンツの所有者／配布者は、配布者として示す。ディジタルコンテンツの購入者／利用者は、利用者として示す。利用者が購入したディジタルコンテンツを盗もうとするクラッカーは、クラッカーとして示す。

【００２７】次に、図１に、この発明に係る汚染プログラムは配布実行方式及び汚染プログラム配布実行方法を実現するシステムのブロック図の一例を示す。図１に示すシステムでは、汚染プログラム配布装置１と汚染プログラム実行装置２と配信用公開鍵登録・公開ステーション３とから構成されている。オリジナルプログラムに対する汚染の実施とその浄化情報の生成は、事前に実行済みとして説明する。また、ここでは、オリジナルプログラムを汚染する工程については、説明を省略する。汚染プログラム配布装置１は、この汚染された汚染プログラムを配布する装置である。汚染プログラム配布装置１は、以下の構成を有する。２１は、予め汚染されたプログラムを記憶する配布汚染プログラム記憶部である。２２は、予め定められている汚染プログラムの汚染された所定の部分で汚染される元の状態に浄化するための浄化

8

情報を記憶する浄化情報記憶部である。上記浄化情報は、汚染された所定の部分の場所を特定する情報（判別鍵）と、汚染された所定の部分を浄化する情報（汚染値）と含む情報である。この実施の形態では、汚染値は、定数Ｙの値を一例として説明する。しかし、汚染値は、定数に限られることなく、プログラムを汚染する値であれば、その他の値であってもよい。例えば、乱数を用いて汚染値を決めても構わない。５は、浄化情報を予め定められている配布先利用者の暗号鍵を用いて暗号化する浄化情報暗号化部である。以下では、浄化情報を暗号化する暗号鍵を配信用公開鍵といい、配信用公開鍵登録・公開ステーション３の中の配信用公開鍵記憶部４から取り出して使うものであり、後述する。６は、汚染プログラムと浄化情報暗号化部５が暗号化した浄化情報とを配信する配信部である。

【００２８】配信用公開鍵登録・公開ステーション３は、浄化情報を暗号化する配信用公開鍵を登録及び公開するステーションである。配信用公開鍵登録・公開ステーション３は、各利用者個別に割り当てられる公開暗号鍵としての配信用公開鍵を記憶する配信用公開鍵記憶部４を備える。４の中には、浄化情報を暗号化する際に使用する利用者の配信用公開鍵がリストされており、その中から配布先利用者の配信用公開鍵を索引する。この配信用公開鍵は、認証用公開鍵とは別に、利用者個別に割り当てられた電子配信用公開鍵である。この実施の形態では、利用者の配信用公開鍵は、一例としてＲＳＡ公開鍵を使用する。しかし、これに限るわけではなく、この他のものでも構わない。

【００２９】汚染プログラム実行装置２は、汚染プログラム配布装置１から配布された汚染プログラムを受信し、汚染プログラムを汚染されたまま実行開始するとともに、汚染された所定の部分を実行する場合に、汚染された所定の部分を汚染される元の状態に浄化して実行する装置である。汚染プログラム実行装置２は、以下の構成を有する。７は、汚染プログラムと暗号化された浄化情報とを汚染プログラム配布装置から受信する受信部である。８は、受信部７が受信した汚染プログラムを記憶する汚染プログラム記憶部である。２０は、受信部７が受信した暗号化された浄化情報を記憶する暗号化浄化情報記憶部である。９は、汚染プログラム記憶部８から汚染プログラムを入力して実行するプログラム実行部である。１０は、暗号化浄化情報記憶部２０から暗号化された浄化情報を入力し、暗号化された浄化情報を復号するとともに、プログラム実行部９の汚染プログラムの実行中に、浄化された浄化情報に基づいて汚染プログラムの汚染された所定の部分を特定し、特定した所定の部分を浄化してプログラム実行部９に実行させる動的浄化機構である。３４は、命令レジスタである。３５は、プログラムの実行状態を示すＰＳＷ（Ｐｒｏｇｒａｍ　ＳｔａｔｕｓＷｏｒｄｓ）である。３６は、命令デコーダであ

9

り、３７は、論理演算装置（ＡＬＵ：Ａｒｉｔｈｍｅｔｉｃ　Ｌｏｇｉｃ　Ｕｎｉｔ）である。

【００３０】更に、動的浄化機構１０は、以下の１１～１６の構成を有する。１１は、暗号化された浄化情報を復号するための復号鍵である利用者受信用秘密鍵（以下、「利用者受信用秘密鍵」を「受信用秘密鍵」という）を記憶する受信用秘密鍵レジスタ（ＫＲ）である。即ち、受信用秘密鍵レジスタ（ＫＲ）１１は、汚染プログラム配布装置１の浄化情報暗号化部５において、配信用公開鍵によって暗号化された浄化情報を復号する受信用秘密鍵を記憶する。１２は、受信用秘密鍵レジスタ（ＫＲ）１１に記憶された受信用秘密鍵を用いて暗号化された浄化情報を復号する浄化情報復号部である。１３は、浄化情報復号部１２により復号された浄化情報により復号された浄化情報を保持する浄化情報レジスタ（ＨＲ）である。また、浄化情報レジスタ（ＨＲ）１３は、汚染された所定の部分の場所を特定する情報を記憶する判別鍵レジスタ（ＤＲ）１８と、汚染された所定の部分を浄化する情報を記憶する汚染値レジスタ（ＣＲ）１９とを含む。１４は、プログラム実行部９により実行された実行情報を保持する実行情報レジスタ（ＩＲ）である。１５は、浄化情報レジスタ（ＨＲ）１３の判別鍵レジスタ（ＤＲ）１８に保持された浄化情報と実行情報レジスタ（ＩＲ）１４に保持された実行情報とを比較する比較部である。１６は、比較部１５の比較の結果に基づいて、浄化情報を用いて汚染プログラムの汚染された所定の部分を浄化する浄化部である。この実施の形態では、浄化部１６は、汚染されていたオペランドを元に戻す汚染除去器である。以下の説明では、汚染除去器１６、もしくは、浄化部１６と表現するが、同じ意味で使用する。

【００３１】汚染プログラム配信実行方式及び方法の動作の概略を図１，図２を用いて説明する。利用者は、配布者にプログラム配布要求を通知する。配布者は、汚染プログラム配布装置１を使用するに当たって、必要な事項を予め定義する等の準備を行う（Ｓ１１）。必要な事項とは、汚染値やプログラムの汚染場所、暗号化、復号のための鍵などを決定する。決定した項目に基づいてプログラムを汚染し、汚染した汚染プログラムを配布汚染プログラム記憶部２１へ格納する。また、汚染したプログラムを浄化する浄化情報を浄化情報記憶部２２へ格納する。汚染プログラム配布装置１は、配布汚染プログラム記憶部２１から配布の対象となる汚染プログラムを読み出し、配信部６へ出力する（Ｓ２１）。同時に、浄化情報を読み出し、浄化情報暗号化部５へ出力する（Ｓ２２）。浄化情報暗号化部５は、浄化情報の暗号化を行う（Ｓ２２）。暗号化した浄化情報は、汚染プログラムとともに配信部６へ出力する。配信部６は、汚染プログラム実行装置２へ暗号化された汚染プログラムと暗号化浄化情報とを送信する（Ｓ２３）。

10

【００３２】汚染プログラム実行装置２は、配信部６から送信された汚染プログラムと暗号化浄化情報とを受信部７によって受信し、汚染プログラム記憶部８と暗号化浄化情報記憶部２０へそれぞれ出力する（Ｓ３１）。プログラム実行部９は、汚染プログラム記憶部８に記憶された汚染プログラムを汚染されたまま実行開始するとともに、汚染された所定の部分を実行する場合に、動的浄化機構１０によって、汚染された部分を汚染される元の状態に浄化して実行する（Ｓ３２）。詳細は、後述する。以上が、動作の概略である。

【００３３】次に、プログラムの汚染方式を説明する。図３に、プログラムの汚染方式を模式的に示す。まず、配布者が予め定めることを説明する。配布者は、命令語（機械語命令）１語分（一命令分）の長さの定数Ｙを汚染値として用意する。一旦、あるプログラムに対して定数Ｙを決めたなら、同一のプログラムに対して定数Ｙは固定される。このようにして、同一のプログラムには、同一の汚染方式を施す。配布者は、プログラム中で、汚染する場所を一箇所選ぶ。一箇所とは、連続したｎ語の命令であり、プログラムの実行段階でそのｎ語の命令が一意固定的に順次実行される箇所であることが条件となる。図３では、「先行命令」と表した部分がｎ語の命令の部分に当たる。以下、ｎ語の命令を「ｎ語先行命令」、もしくは、「先行命令群」という。実際に汚染が施されるのは、ｎ語の次の命令Ｘのオペランド部分となる。ｎの値は、汚染する命令語が特定できる範囲において任意に定めて構わない。

【００３４】プログラム配布者は、プログラムをインターネットで配布する前に、プログラムのメインルーチンのある１個所の命令語を選ぶ。ここでは、命令Ｘを選択することとする。その命令ＸのオペランドＰを変形する。即ち、これが汚染に当たる。この場合、命令Ｘに先立つｎ個の命令のシーケンスが実行状況によって変動しないような場所を選択する。また、命令ＸのオペランドＰが実行の状況によって変動しないものを選択する。なお、この汚染は、対象プログラムによって一定場所、一定定数とする。ユーザ毎に別の汚染を施すことは、労力が大変な上に、複数ユーザの結託によるバイナリ比較により、汚染場所を容易に発見される恐れがあるため、このような方式を使用する。

【００３５】なお、命令（機械語命令）中のオペレーションコードの排他的論理和をとった結果が未使用のオペレーションコードとなる場合があり得る。この場合、実行形式プログラムを逆アセンブルすることにより、汚染を施した箇所が見つけられる恐れが生じる。これに対処するためには、プログラムの汚染は、命令中のオペランド部分に対して施すようにするなどの対処が考えられる。この際にも、重要なデータを記憶するメモリを破壊する恐れの有無を考慮する必要が生じることになる。

【００３６】配布者が予め定めた定数Ｙとｎ語先行命令

は、配布者のみが秘密裡に管理すべき汚染情報であり、汚染を除去しオリジナルプログラムに浄化する為に必要な情報でもある。従って、この汚染情報が浄化情報となる。また、仮に、ｎ語先行命令とまったく同じ内容でｎ語連続する命令ステップがプログラムの別の場所に存在すれば、配布者は、その場所の次の命令のオペランド部分も同様に汚染しておかねばならない。

【００３７】配布者は、このプログラムを配信すべき利用者がいかに多人数であろうとも、同じオリジナルプログラムに対して、異なる利用者毎に汚染値を変えることはない。配布者は、すべての利用者に同じ汚染プログラムを配信する。図４に一例を示すように、汚染プログラム及び配信用公開鍵で暗号化された浄化情報とは、ユーザＡ、ユーザＢに送られる場合、同じ汚染プログラム及びユーザＡ、ユーザＢ各個別の配信用公開鍵で暗号化した浄化情報が配布される。汚染プログラム実行装置２内の処理は、後述する。

【００３８】次に、配布者は、利用者に対して汚染したプログラムを配送する。そのとき、同時に汚染場所を見つけるためのｎ個の先行命令と汚染したオペランドを浄化するための定数Ｙとを浄化情報として添付して配送する。しかし、この汚染浄化情報が盗まれたり、コピーされたりすると、対象プログラムを汚染していることの意味がなくなる。そこで、配布者は、浄化情報をそのまま配送することはせず、利用者の配信用公開鍵で暗号化し、これを暗号化浄化情報として配送する。この結果、配布者がユーザへ配布するプログラムは、全て同一バイナリ形をしているが、浄化情報は、ユーザ毎に別々に暗号化されたバイナリ形となる。プログラムは、一般に膨大な情報量である。これを同一バイナリ形で送る。一方、ユーザ毎に異なる形となる暗号化浄化情報は、情報量としてプログラムに比べると非常に小さい。ユーザは、受け取った汚染プログラムの浄化情報を自分の受信用秘密鍵で復号したときだけ正しく浄化することができる。

【００３９】利用者は、汚染プログラムと浄化情報を受け取ると、プログラムを走行させる前に、浄化情報を自己の受信用秘密鍵で復号する。図４に示す汚染プログラム実行装置２に、この模式図を示している。これによって、本来の浄化情報を得る。なお、動作を理解しやすいように、かかる準備動作を利用者自身が行うかのように説明しているが、これらは配布された汚染プログラム自身が呼び出されたときに自動的に行うことも可能である。このように、浄化情報のみがユーザ毎の配信用公開鍵により個別に暗号化され、配信される。汚染プログラムはどのユーザに対しても同一のものが送られる。従って、複数のユーザが共謀して送られてきた汚染プログラムをバイナリ比較しても、汚染箇所を同定することはできない。

【００４０】次に、動的浄化機構１０を実現するために必要となるＣＰＵ（ＣｅｎｔｒａｌＰｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）の拡張について説明する。具体的には、汚染プログラムの動的浄化、即ち、汚染プログラムを実行しながら、汚染箇所の浄化を行うために汚染プログラム実行装置２のＣＰＵの拡張、即ち、機能の付加について説明する。動的浄化機構１０は、３組のレジスタ（ＫＲ，ＨＲ，ＩＲ）群を主とするハードウェアであり、既存のプロセッサの上に追加するものである。

【００４１】図５に、動的浄化機構１０及び関連するプログラム実行部９のブロック図を示す。図１と同じ符号を付けたものは、同一の構成要素である。汚染プログラム実行装置２側の動的浄化機構１０内に隠蔽される特別なレジスタを用意する。このレジスタを「セキュアレジスタ」とする。図１及び図５のＫＲ１１，ＨＲ１３（ＤＲ１８，ＣＲ１９を含む），ＩＲ１４が該当する。このセキュアレジスタは、既存の機械語命令ではアクセスできないものとし、更に、セキュアレジスタの内容を主記憶上や他の装置へ読み出す機械語命令は用意されないことを前提とする。従って、セキュアレジスタ内のデータを覗くことはできないことになる。

【００４２】予め定められた各利用者の配信用公開鍵で暗号化されている浄化情報を復号して、その結果をセキュアレジスタに格納する命令を用意する。そこで、ＤｅｃｒｙｐｔＳＲ命令を新設する。ＤｅｃｒｙｐｔＳＲは、ファームウェアで実装される命令であり、セキュアレジスタＫＲへ格納されている受信用秘密鍵を使用して一連の復号計算を行う。しかし、あくまで一個の命令であり、復号結果及び復号途中のデータは、主記憶上には一切残らない。この命令は、浄化情報を受信用秘密鍵によって復号したデータをＨＲへ格納するために使用する。具体的には、ｎ語先行命令をＫＲに記憶する受信用秘密鍵により復号計算して、結果をＨＲ内のＤＲへ格納する。また、受信用秘密鍵によって同様にして復号した汚染値（定数Ｙ）をＨＲ内のＣＲへ格納する。ＨＲ内のＤＲ及びＣＲにデータセットする手段は他には用意しない。また、ここでは、受信用秘密鍵により復号した浄化情報をこのような特殊なレジスタＨＲへのセットに限定して使用する。このため、ここでいう受信用秘密鍵と新たに定義したＤｅｃｒｙｐｔＳＲ命令とは、個人認証用には使用できないことになる。従って、個人認証用の秘密鍵（図示していない）は、受信用秘密鍵とは別に持つ必要がある。ここでの受信用秘密鍵は、いわばディジタルコンテンツのセキュア流通用の専用鍵である。

【００４３】図６に、セキュアレジスタ群の動作の詳細を示している。セキュアレジスタＨＲは、ＤｅｃｒｙｐｔＳＲ命令によって設定される。動的浄化機構１０は、セキュアレジスタである利用者の受信用秘密鍵レジスタＫＲ（Ｋｅｙ　Ｒｅｇｉｓｔｅｒ，ＫＲ）を１個保有する。ＫＲには、利用者のの受信用秘密鍵を格納する。ＫＲに受信用秘密鍵をセットするための命令としてＬｏａ

ｄ　Ｋｅｙ命令を新設する。Ｌｏａｄ　Ｋｅｙ命令は、利用者の個人情報等を記憶するＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）カードから受信用秘密鍵を読み、直接ＫＲへ格納する。Ｓｔｏｒｅ　Ｋｅｙ命令は作らない。従って、ＫＲ内の受信用秘密鍵を主メモリへ読み出す手段はないことになる。

【００４４】動的浄化機構１０は、セキュアレジスタであるＨＲ（Ｈｉｄｄｅｎ　Ｒｅｇｉｓｔｅｒ，ＨＲ）は、ｎ個のＤＲと１個のＣＲを保有する。この実施の形態では、ｎを汚染命令Ｚを識別するための先行命令の数とする場合を示している。また、先行命令に汚染値（定数Ｙ）を加えた情報を浄化情報としているため、ｎ＋１となっている。ＨＲの語長は、ホストのマイクロプロセッサの語長に一致させる。ＤｅｃｒｙｐｔＳＲにより浄化情報が復号された際に、定数Ｙが格納されるセキュアレジスタの一つを汚染値レジスタ（ＣＲ）１９とし、汚染された所定の部分の場所を特定する情報として、ｎ語先行命令が格納されるセキュアレジスタ群を判別鍵レジスタ（ＤＲ）１８とする。また、判別鍵レジスタ（ＤＲ）１８と汚染値レジスタ（ＣＲ）１９とを浄化情報レジスタ（ＨＲ）１３として、浄化情報を記憶するレジスタとしている。

【００４５】実行情報レジスタ（ＩＲ）１４は、プログラム実行中に、過去ｎ語分の命令を保持するためのセキュアレジスタ群として使用する。実行情報レジスタ（ＩＲ）１４は、シフトレジスタ構成を採っており、過去ｎ語分の命令をＦＩＦＯ（Ｆｉｒｓｔ－Ｉｎ　Ｆｉｒｓｔ－Ｏｕｔ）式に保存する。

【００４６】ｎ個のＩＲ（ＩＲ１～ＩＲｎ）について説明する。マイクロプロセッサにおいて、実行する命令（Ｃｕｒｒｅｎｔ　Ｉｎｓｔｒｕｃｔｉｏｎ）をフェッチすると、その命令語を命令レジスタへセットすると同時に、ＩＲ１へもセットする。その後、機械語命令が１語フェッチされる都度、ＩＲはＣｕｒｒｅｎｔ　Ｉｎｓｔｒｕｃｔｉｏｎを受け取り、古い命令は順次ＩＲ１→ＩＲ２→ＩＲ３→・・・→ＩＲｎへと渡されていく。結果として、ＩＲの中には、Ｃｕｒｒｅｎｔ　Ｉｎｓｔｒｕｃｔｉｏｎから過去へ遡ったｎ個の命令のシーケンスがいつも垂れ流し的に存在する。但し、ＩＲがこのような動作を行うのは、ある特定のプログラムの実行中とする。特定のプログラムであるか否かはＰＳＷが判断する。その特定のプログラムが他のプログラムに割り込まれて走行休止中は、ＩＲへの命令の受け渡しも休止する。

【００４７】次に、図５の比較部１５について説明する。比較部１５は、比較器３８と汚染除去フラグ３９を有する。比較器３８は、判別鍵レジスタ（ＤＲ）１８の内容と実行情報レジスタ（ＩＲ）１４の内容を比較し、両者の一致を検出する回路である。比較器３８が一致を検出すると汚染除去フラグ３９をセットする。汚染除去フラグ３９は、一致を検出した命令の次の命令を実行する際に、汚染除去動作を行うように次に命令の実行時間帯に指示を与えるフラグである。汚染除去フラグ３９も、セキュアレジスタである。

【００４８】更に、汚染除去器１６は、命令レジスタ３４の内容が命令デコーダに送られる経路に付加される。汚染除去器１６は、命令レジスタ３４の内容と汚染値レジスタ（ＣＲ）１９に格納されている定数Ｙとの排他的論理和をとる機構である。

【００４９】上記のＣＰＵの拡張は既存のいかなるマイクロプロセッサに対しても、上位互換的に可能である。換言すれば、動的浄化機構の実現は既存のプロセッサの改良で足りるものであり、また、動的浄化機構が追加されたプロセッサは、現状機種との上位互換性が完全に保証される。

【００５０】次に、汚染プログラム実行装置２内の動的浄化機構の動作の詳細について図１，図５及び図６を用いて説明する。まず、汚染プログラム実行装置２は、該当プログラムを実行する際に、ＤｅｃｒｙｐｔＳＲ命令を実行して浄化情報を復号する。この結果、浄化情報（定数Ｙ及びｎ語先行命令）がそれぞれ汚染値レジスタ（ＣＲ）１９と判別鍵レジスタ（ＤＲ）１８に格納される。

【００５１】汚染プログラム記憶部８から命令が読み出され、命令レジスタ３４と実行情報レジスタ（ＩＲ）１４に格納される。実行情報レジスタ（ＩＲ）１４には、実行する命令がＦＩＦＯ式に保存される。実行情報レジスタ（ＩＲ）１４にｎ語先行命令のすべてが保存されるまでは、判別鍵レジスタ（ＤＲ）１８と実行情報レジスタ（ＩＲ）１４の内容は一致しないため、比較器３８からは０（零）が出力される。この結果、命令レジスタ３４内の命令がそのまま実行される。当該プログラムが走行している間は、動的浄化機構１０内のＩＲには常に直近のｎ個の命令が順番にシフトを繰り返しつつ格納されている。そのうちに、オペランドを汚染した直前の命令がＩＲ１に受け渡されるときがやってくる。このとき、ＤＲの中に格納されている本来の浄化情報とＩＲとを比較すると、（ＤＲ１）＝（ＩＲ１），（ＤＲ２）＝（ＩＲ２），・・・，（ＤＲｎ）＝（ＩＲｎ）が成立する。この結果、判別鍵レジスタ（ＤＲ）１８の内容（ｎ語先行命令）と実行情報レジスタ（ＩＲ）１４の内容（現命令より過去ｎ語分の命令）が一致し、比較器３８から１が出力される。これを受け、汚染除去フラグ３９がセットされる。除去フラグがセットされると、その次の命令の実行時間帯にスイッチ４０を切り換えるように制御する。

【００５２】次に、汚染命令Ｚが命令レジスタ３４に読み込まれる。命令レジスタ３４内では、汚染命令Ｚは汚染されたままの状態で読み込まれる。しかし、この段階で汚染除去フラグ３９がセットされているため、命令レ

ジスタ３４の内容は、命令デコーダ３６のゲート群へ送られる途中で汚染除去器１６により汚染が除去され、命令デコーダ３６に届く。汚染除去器１６では、ＣＲに記憶されている定数Ｙと汚染命令Ｚとの排他的論理和を取る。この結果、汚染されたオペランドは、デコーダに入る寸前に正しいデータへ浄化される。この結果、汚染命令Ｚは、ＣＰＵにより実行される直前にオリジナルプログラムの命令Ｘに動的浄化機構によって動的浄化され、プログラムは正しく実行される。

【００５３】図７に、汚染プログラムと浄化情報の暗号化、復号に伴うコンテンツの流れを示している。汚染プログラム配布装置では、汚染プログラムと配信用公開鍵によって暗号化された浄化情報とが、汚染プログラム実行装置２へ転送される。汚染プログラム実行装置２では、まず、浄化情報が受信用秘密鍵によって復号され、その結果得られた、復号された浄化情報を用いて、汚染プログラムを動的浄化しながら実行する。浄化情報は、前述したように、受信用秘密鍵によって復号されがとき、外部から覗かれぬようセキュアレジスタへ設定される。

【００５４】浄化情報は、配信用公開鍵によってＲＳＡ暗号方式で暗号化されているため、その復号には時間がかかる。しかし、浄化情報は該当プログラムの実行前に前もって復号されるものであるので、プログラムの実行速度を侵害することはない。一方、動的浄化機構１０によって行う動的浄化は、排他的論理和により実現される。排他的論理和の機構はたかだか論理ゲート２段の追加で実現できるので、プログラムの実行速度に影響を及ぼすことはない。復号された状態の浄化情報は、セキュアレジスタ内にしか存在しない。前述したように、セキュアレジスタの内容を読み出す機械語命令は用意されておらず、クラッカーや利用者が浄化情報を盗み出すことは不可能である（ＬＳＩのパッケージを解いて、プロービングするしかない）。

【００５５】なお、プログラム中に条件付きジャンプがある場合、実行時の条件によってプログラムの実行経路が異なり、実行情報レジスタ（ＩＲ）１４に格納される過去ｎ語分の命令が変わってくる。よって、条件付きジャンプに関わる箇所をｎ語先行命令に選ぶことは避ける。同様の理由で、プログラム実行中に他の命令によってオペランドなどが書き換えられる可能性のある箇所もｎ語先行命令としてはいけない。また、プログラム中にｎ語先行命令と同一となっている命令群が複数存在する場合、すべての箇所の次命令に汚染を施す必要がある。

【００５６】また、上記説明は、１ステップの命令がすべて１語で統一されている場合には判り易いが、可変長命令に対しても対応可能である。ただし、命令語長が可変の場合、ｎ語からなる判別鍵レジスタ（ＤＲ）１８にｎステップの命令が収まるとは限らず、命令ステップ数としてはｎ以下となる。また、ｎ語先行命令内の最終命令の後半部がｎ語の判別鍵レジスタ（ＤＲ）１８からあふれるケースも起こり得る。しかし、その時点では実行情報レジスタ（ＩＲ）１４側も同様に、最後の一部があふれて失われているから、比較部１５において、一致検出するに当たっては支障はない。

【００５７】以上のように、この発明に係る汚染プログラム配布実行方式は、或る一つのプログラムを独立複数の利用者のそれぞれの汚染プログラム実行装置へ個別に配布する場合にすべての利用者に対し同一の汚染を行った汚染プログラムと、汚染プログラムの汚染に対応する同一の浄化情報を各利用者が各個に保有する公開暗号鍵で各個に暗号化した暗号化浄化情報とを組み合せて配布することを特徴とする。

【００５８】このようにして、この汚染プログラム配布実行方式は、汚染プログラムに如何に手を掛けずににリピータブルに多数のユーザへ同じプログラムを配布するかという問題を解決するものである。汚染プログラム配布装置１から配布する二つの情報として、汚染プログラムと、暗号化浄化情報との大きさを比較した場合に、汚染プログラムに比べて暗号化浄化情報は遥かに小さい。そこで、この汚染プログラム配布実行方式は、汚染プログラムを一式用意するとともに、各利用者毎に暗号化浄化情報を用意することによって、同じ汚染プログラムをすべてのユーザに配布することを可能にする方式である。

【００５９】実施の形態２．この実施の形態では、マルチタスクへ対応する場合について説明する。汚染プログラム実行装置２において、複数のプログラムが同時に実行される場合、ＣＰＵは現タスクに関する情報をすべてスタックに退避した上で、次のタスクの実行に移る必要がある。汚染プログラムの動的浄化機構１０には、いくつかのセキュアレジスタが存在するが、タスク切り替え時にセキュアレジスタの内容がスタック（主記憶）に積まれてしまっては、浄化情報が漏洩する原因になりかねない。従って、この発明に係る汚染プログラム配布実行方式をマルチタスクへ対応させるためには、同時に実行するタスクの数だけセキュアレジスタ群を用意する必要がある。同時に実行するタスクの数をｍとすると、汚染プログラム実行装置２は、ｍ式のセキュアレジスタ群を備える必要がある。但し、ＫＲは全体に共通に１個だけ設けるものなので除外する。更に、ＰＳＷ（Ｐｒｏｇｒａｍ　Ｓｔａｔｕｓ　Ｗｏｒｄｓ）３５に数ビットのセキュアレジスタ群指示フラグを用意する。ＰＳＷは、現在実行中のタスクが何番目であるかをセキュアレジスタ群指示フラグへ記憶する。また、ｉ番目のタスクには、ｉ番目のセキュアレジスタ群を対応させるものとする。このようにして、タスクと動的浄化機構１０を対応付ける。

【００６０】ＣＰＵは、現在何番目のタスクが実行されているかの情報を、ＰＳＷ３５のセキュアレジスタ群指

示フラグに設定する。動的浄化機構１０は、ＰＳＷ３５のセキュアレジスタ群指示フラグの情報を基に、自分がいつ動作すべきかを知ることができる。例えば、ｉ番目のタスクが実行されているときには、ＰＳＷ３５のセキュアレジスタ群指示フラグはｉ番を示し、それにより、ｉ番目の動的浄化機構１０が活性化され、該当タスクに対するプログラムの動的浄化を行う。

【００６１】実施の形態３．この実施の形態では、割り込み処理への対応を説明する。割り込みが発生した場合、ＣＰＵは実行中のプログラムを一旦停止し、割り込み処理を開始する。この結果、実行情報レジスタ（ＩＲ）１４には、割り込み処理ルーチンの命令（機械語命令）が格納されてしまうことになる。従って、先行命令群に対応する機械語命令が実行されている途中で割り込みが発生した場合、実行情報レジスタ（ＩＲ）１４の内容と判別鍵レジスタ（ＤＲ）１８が一致しなくなってしまう。上記の問題も実施の形態２で説明したＰＳＷの拡張機能が解決することになる。汚染プログラム実行装置２のプログラム実行部９は、汚染プログラムを実行する。該当プログラムが走行開始する前に、ＰＳＷの所定のセキュアレジスタ群指示フラグがセットされる。動的浄化機構１０は、それを見て指示フラグ該当群のＩＲがＬａｔｅｓｔ Ｉｎｓｔｒｕｃｔｉｏｎの受け取りとシフトを開始する態勢に入る。該当プログラムが他のプログラムに割り込まれたときは、ＰＳＷの所定のセキュアレジスタ群指示フラグが別物に変わるから、該当動的浄化機構１０は休止する。このとき、ＰＳＷの所定のセキュアレジスタ群指示フラグが別のセキュアレジスタ群の番号を指定していれば、別のセキュアレジスタ群が動作態勢に入る。割り込み処理ルーチン実行中は、ＰＳＷ３５のセキュアレジスタ群指示フラグは立たない。従って、実行情報レジスタ（ＩＲ）１４は、ｄｉｓａｂｌｅとなり、機械語命令の格納を停止する。割り込み処理が終了した後には、再びＰＳＷ３５のセキュアレジスタ群指示フラグが該当番号となるので、該当実行情報レジスタ（ＩＲ）１４がｅｎａｂｌｅとなり機械語命令の格納を再開する態勢に入る。図１に示す例では、ＰＳＷ３５の下のスイッチによってｄｉｓａｂｌｅ又はｅｎａｂｌｅを指示している。

【００６２】特殊なタイミング条件として、汚染プログラムの汚染命令Ｚの実行寸前に割込みが入ることも起こり得る。この場合は、先行ｎ語命令の比較一致が成立し、除去フラグが立った直後に割込みが発生することになる。この場合は、割込みに伴うＰＳＷ変更がハードウェアによって実施され、それに続いて、割り込み処理ルーチンの先頭命令の実行に入る。そこで、先に立っていた除去フラグが、もし、この先頭命令で有効となると、汚染命令Ｚではない部分で誤った汚染浄化を行うこととなる。この誤動作を避けるため、除去フラグも、また、セキュアレジスタ群の一員として、ＰＳＷ変更のときに別の除去フラグに切り換わることとする。割込ルーチンが終了するとき、先に立っていた除去フラグがＰＳＷとともに回復され、その後に汚染命令Ｚが実行され、汚染浄化が予定通り実施される。

【００６３】

【発明の効果】この発明に係る汚染プログラム配布実行方式及び汚染プログラム配布実行方法によれば、汚染プログラムを流通させるため、オリジナルのプログラムの不正コピーを防止することができる。

【００６４】この発明によれば、汚染プログラムと浄化情報を受け取ることにより、オリジナルプログラムを記憶装置に残すことなく汚染プログラムを実行することができる。

【００６５】この発明によれば、汚染プログラムと浄化情報により実行直前にプログラムの汚染部分を浄化することが可能になり、正常にプログラムを実行することができる。

【００６６】この発明によれば、浄化情報を外部に漏らすことを防止することができる。

【００６７】この発明によれば、浄化情報により、配布者が汚染したプログラムを浄化することができる。

【００６８】この発明によれば、実行中の先行命令を検索することにより、プログラムの汚染部分を特定することができる。

【００６９】この発明によれば、マルチタスクの装置へも適用することができる。

【００７０】この発明によれば、第三者が汚染プログラムを不正取得してもプログラムの正常な実行を不可能とすることができる。

【００７１】この発明によれば、第三者が汚染プログラム及び或る利用者の暗号化浄化情報の双方を不正取得しても、第三者の実行装置の上ではプログラムの正常な実行を不可能とすることができる。

【００７２】この発明によれば、同一のプログラムでは、同一の汚染プログラムを配布するため、プログラムの汚染箇所、汚染方式の検出を防ぐことができる。

【００７３】この発明によれば、汚染プログラムを同一のバイナリ形式で複数の利用者へ配布することにより、プログラム配布の手間・費用を低く押さえることができる。

【図面の簡単な説明】

【図１】　この発明の実施の形態１の汚染プログラム配布実行方式の一例を表わすブロック図である。

【図２】　この発明の実施の形態１の汚染プログラム配布実行方式及び方法の動作のフロー図である。

【図３】　この発明の実施の形態１の汚染プログラム配布実行方式及び方法のプログラムの汚染方法の詳細を表わした図である。

【図４】　この発明の実施の形態１の汚染プログラム配布実行方式及び方法の汚染プログラムの配布の方式の一

例を表わした図である。

【図５】　この発明の実施の形態１の汚染プログラム配布実行方式及び方法の動的浄化機構の詳細の一例を表わした図である。

【図６】　この発明の実施の形態１の汚染プログラム配布実行方式及び方法の動的浄化機構のセキュアレジスタ群の動作の一例の詳細を表わした図である。

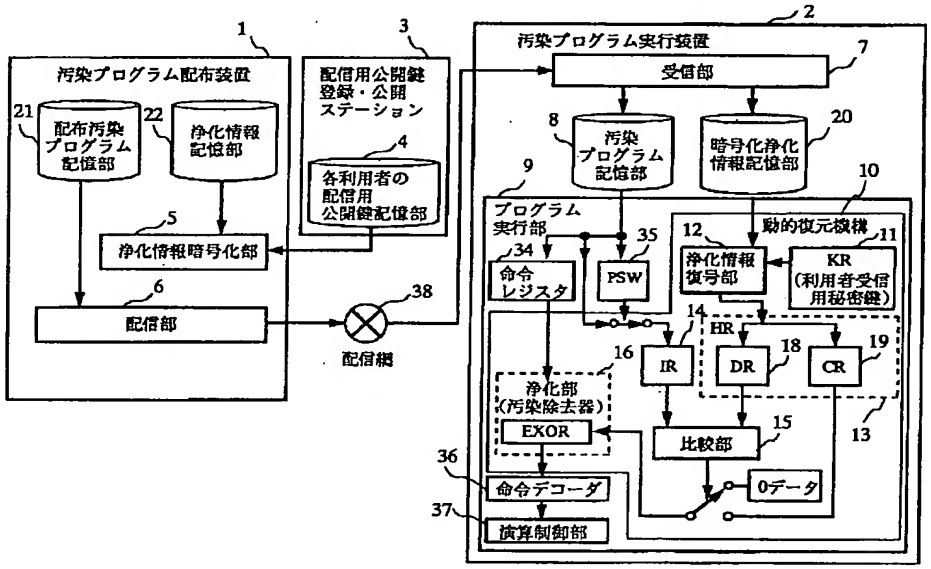
【図７】　この発明の実施の形態１の汚染プログラム配布実行方式における汚染プログラムと浄化情報との暗号化、復号に伴うコンテンツの流れを示した図である。

【図８】　従来のオリジナルコンテンツを利用した流通を表した図である。

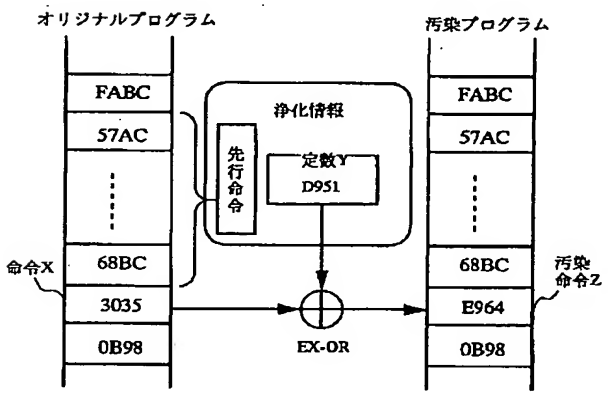
【符号の説明】

１　汚染プログラム配布装置、２，２ａ，２ｂ　汚染プログラム実行装置、３配信用公開鍵登録・公開ステーション、４　各利用者配信用公開鍵記憶部（配信用公開鍵記憶部）、５　浄化情報暗号化部、６　配信部、７　受信部、８　汚染プログラム記憶部、９　プログラム実行部、１０　動的浄化機構、１１　受信用秘密鍵レジスタ（ＫＲ）、１２　浄化情報復号部、１３　浄化情報レジスタ（ＨＲ）、１４　実行情報レジスタ（ＩＲ）、１５　比較部、１６　浄化部（汚染除去器）、１８　判別鍵レジスタ（ＤＲ）、１９　汚染値レジスタ（ＣＲ）、２０　暗号化浄化情報記憶部、２１　配布汚染プログラム記憶部、２２　浄化情報記憶部、３４　命令レジスタ、３５　ＰＳＷ、３６　命令デコーダ、３７　論理演算装置、３８　配信網。

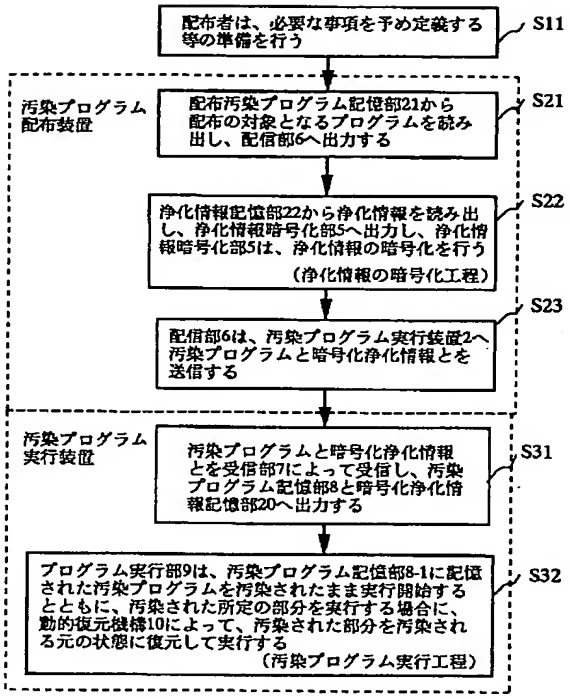
【図１】



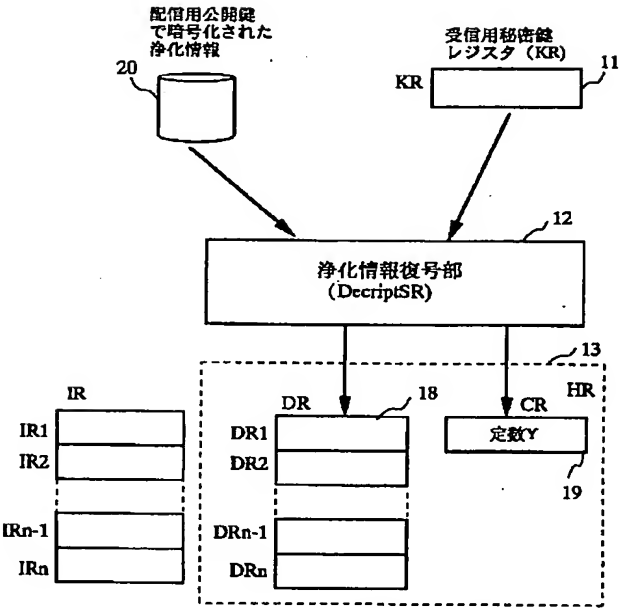
【図３】



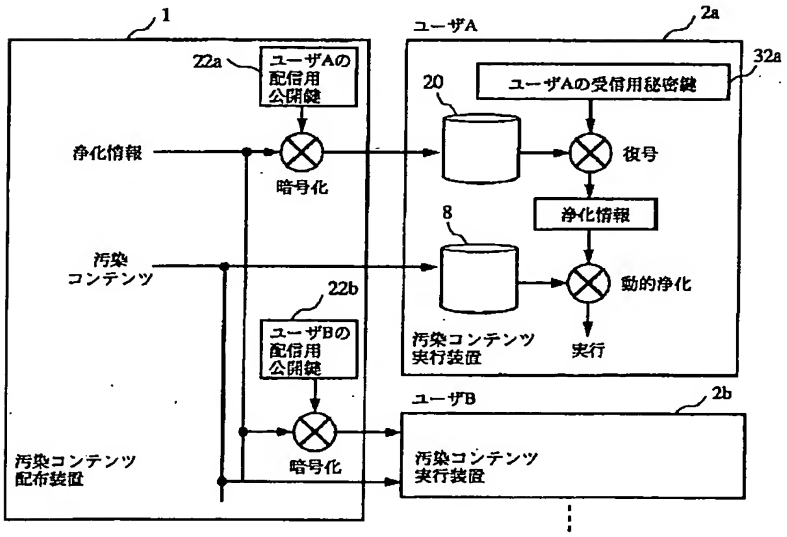
【図２】


配布者は、必要な事項を予め定義する等の準備を行う
S11
汚染プログラム配布装置
配布汚染プログラム記憶部21から配布の対象となるプログラムを読み出し、配信部6へ出力する
S21
浄化情報記憶部22から浄化情報を読み出し、浄化情報暗号化部5へ出力し、浄化情報暗号化部5は、浄化情報の暗号化を行う
（浄化情報の暗号化工程）
S22
配信部6は、汚染プログラム実行装置2へ汚染プログラムと暗号化浄化情報とを送信する
S23
汚染プログラム実行装置
汚染プログラムと暗号化浄化情報とを受信部7によって受信し、汚染プログラム記憶部8と暗号化浄化情報記憶部20へ出力する
S31
プログラム実行部9は、汚染プログラム記憶部8-1に記憶された汚染プログラムを汚染されたまま実行開始するとともに、汚染された所定の部分を実行する場合に、動的復元機構10によって、汚染された部分を汚染される元の状態に復元して実行する
（汚染プログラム実行工程）
S32

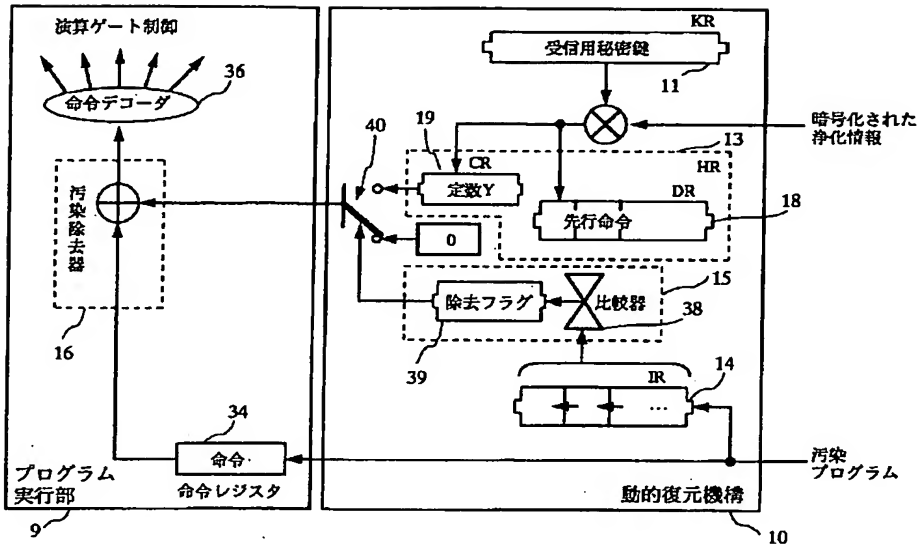
【図６】


配信用公開鍵で暗号化された浄化情報
20
受信用秘密鍵レジスタ（KR）
KR
11
12
浄化情報復号部
(DecriptSR)
13
IR
IR1
IR2
IRn-1
IRn
DR
18
DR1
DR2
DRn-1
DRn
CR
HR
定数Y
19

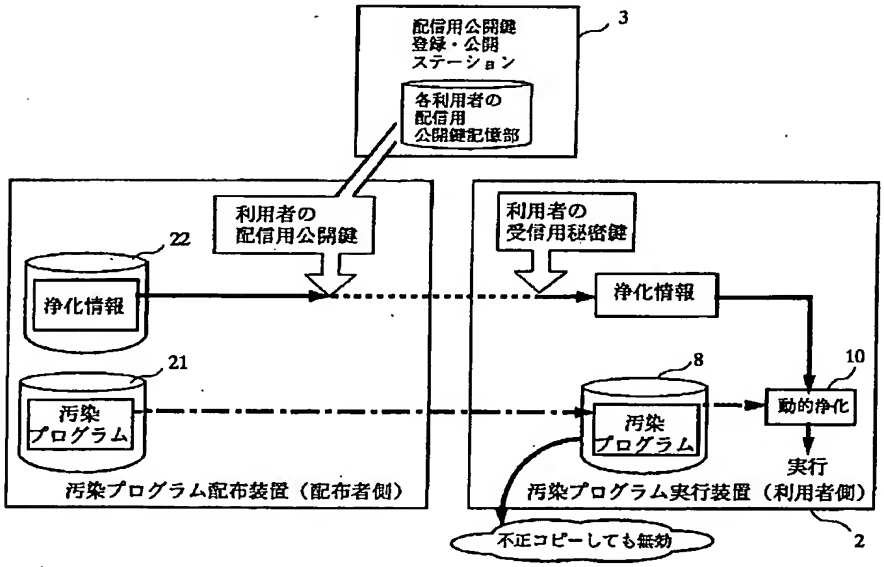
【図４】


1
ユーザA
2a
22a
ユーザAの配信用公開鍵
ユーザAの受信用秘密鍵
32a
20
浄化情報
暗号化
復号
浄化情報
8
汚染コンテンツ
動的浄化
22b
ユーザBの配信用公開鍵
汚染コンテンツ実行装置
実行
ユーザB
2b
暗号化
汚染コンテンツ配布装置
汚染コンテンツ実行装置

【図５】


演算ゲート制御
命令デコーダ
36
汚染除去器
16
プログラム実行部
9
34
命令
命令レジスタ
KR
受信用秘密鍵
11
暗号化された浄化情報
19
40
CR
定数Y
0
13
HR
DR
先行命令
18
除去フラグ
比較器
15
38
39
IR
14
汚染プログラム
動的復元機構
10

【図７】


配信用公開鍵登録・公開ステーション
3
各利用者の配信用公開鍵記憶部
利用者の配信用公開鍵
22
浄化情報
21
汚染プログラム
汚染プログラム配布装置（配布者側）
利用者の受信用秘密鍵
浄化情報
8
汚染プログラム
10
動的浄化
実行
汚染プログラム実行装置（利用者側）
2
不正コピーしても無効

【図８】